(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
20. Dezember 2001 (20.12.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/97525 A1

(51) Internationale Patentklassifikation[7]: H04N 7/24, 5/00

(21) Internationales Aktenzeichen: PCT/EP01/05343

(22) Internationales Anmeldedatum:
10. Mai 2001 (10.05.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
100 296 43.2 16. Juni 2000 (16.06.2000) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **DEUTSCHE TELEKOM AG** [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **EICHENTOPF, Jens** [DE/DE]; Kaiser-Friedrich-Str. 4, D-65193 Wiesbaden (DE). **HEUSER, Stephan** [DE/DE]; Adolf-Spiegel-Str. 1h, D-64409 Messel (DE). **SCHAAF, Christoph** [DE/DE]; Römerstrasse 46, D-64291 Darmstadt (DE). **SCHWENK, Jörg** [DE/DE]; Südwestring 27, D-64807 Dieburg (DE).

(74) Gemeinsamer Vertreter: **DEUTSCHE TELEKOM AG**; Rechtsabteilung (Patente) PA1, D-64307 Darmstadt (DE).

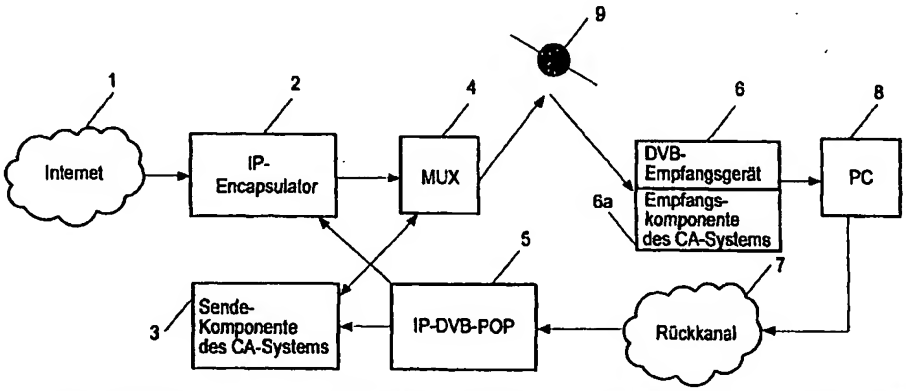
(81) Bestimmungsstaat *(national)*: US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR SECURE TRANSFER OF IP DATA VIA A RADIO MEDIUM

(54) Bezeichnung: VERFAHREN ZUR ABHÖRSICHEREN ÜBERTRAGUNG VON IP-DIENSTEN ÜBER EIN RUNDFUNK-MEDIUM



3...SEND COMPONENT FO CA SYSTEM 6a...RECEIVE COMPONENT OF CA SYSTEM
6...DVB RECEIVER 7...RETURN CHANNEL

(57) **Abstract:** The invention relates to a method for secure transfer of internet protocol services, and IP services, via a radio medium. According to said method, data is divided into DVB transport packets. The DVB transport packets are encrypted by the transmitter of a dedicated device, for example, a multiplexer/MUX (4) or a separate scrambler, transmitted via satellite(9) and decrypted in a DVB receiver 6, for example, a set-top-box STB, a PC plugin card or a DVB server in a LAN. The obtained IP data is then relayed to the corresponding machines/applications such as a PC(8), a router or a TCP/IP-stack.

(57) **Zusammenfassung:** Die Erfindung bezieht sich auf ein Verfahren zur abhörsicheren Übertragung von Internet Protocol-Diensten, IP-Diensten, über ein Rundfunkmedium, bei dem die ankommenden IP-Daten in DVB-Transportpakete aufgeteilt werden. Die DVB-Transportpakete werden dann auf Sendeseite von einem dedizierten Gerät wie beispielsweise einem Multiplexer/MUX (4) oder einem separaten Scrambler verschlüsselt, über einen Satelliten (9) transportiert und auf der Empfangsseite von einem DVB-Empfangsgerät (6), wie beispielsweise einer Set-Top-Box STB, einer PC-Steckkarte oder einem DVB-Server in einem LAN entschlüsselt. Die so erhaltenen IP-Daten werden dann an die entsprechenden Geräte/Applikationen wie einen PC (8), einen Router oder einen TCP/IP-Stack weitergegeben.

WO 01/97525 A1

Veröffentlicht:
— *mit internationalem Recherchenbericht*
— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren zur abhörsicheren Übertragung von IP-Diensten über ein Rundfunkmedium

Beschreibung:

Die Erfindung bezieht sich auf ein Verfahren zur abhörsicheren Übertragung von Internet-Protocol-Diensten, IP-Diensten, über ein Rundfunkmedium gemäß dem Oberbegriff des vorliegenden Patentanspruches.

Der Zugang eines Kunden zum Internet erfolgt heute in der Regel durch Einwahl über eine Punkt-zu-Punkt-Verbindung (Modem, ISDN) in den mit Point of Presence, POP, bezeichneten Zugang eines Internet Service Providers, ISP, wie zum Beispiel T-Online der Deutschen Telekom AG mit Point to Point Protocoll, PPP. Nach Zuweisung einer temporären IP-Adresse an den Kunden wird der gesamte IP-Verkehr von und zu dieser IP-Adresse über die Punkt-zu-Punkt-Verbindung geroutet. Um die Performanz der Anbindung des Kunden an das Internet zu erhöhen, werden einerseits neue Techniken auf der Telefonleitung eingesetzt (z.B. ADSL, T-Online Speed, http://www.t-online.de/service/index/adssvxaa.htm), andererseits werden auch neue bereits vorhandene Übertragungsmedien wie das Breitband Kabelnetz, BK-Kabelnetz und Satelliten eingesetzt (z.B. high-Speed Internet über Satellit, siehe: http://www.astra.lu/multimedia/applications/commercial/high_speed_internet.htm.).

Das BK-Kabelnetz und Satelliten werden bereits in beträchtlichem Umfang zur Verbreitung von digitalem Fernsehen nach den Digital Video Broadcasting-Standards, DVB-Standards (bzw. äquivalenter Standards in den USA und anderen außereuropäischen Staaten) genutzt. Eine besondere Rolle spielt hier Pay-TV. Bei diesem entgeltpflichtigen Dienst werden die Inhalte mit einem Verschlüsselungalgorithmus (z.B. DVB Scrambling Algorithmus, www.dvb.org, oder DES) unter Kontrolle eines Sitzungsschlüssels („Kontrollwort", CW) verschlüsselt übertragen. Der Kunde benötigt eine Set-Top-Box STB mit einem „Conditional Access"-System CA genannten Schlüsselmanagement, um diese Inhalte entschlüsseln

zu können. Dazu wird das Sicherheitsmodul der Set-Top-Box STB (in der Regel eine Chipkarte) mit einer speziellen Nachricht, einer sogenannten „Entitlement Management Message" EMM freigeschaltet. Nach dieser Freischaltung kann dieses andere spezielle Nachrichten, die sogenannten „Entitlement Control Messages" ECM entschlüsseln und die zum Entschlüsseln der Inhalte benötigten Sitzungsschlüssel, die sogenannten „Control Words" CW, ausgeben. (Vgl. auch J. Schwenk, "Conditional Access" oder Wie kann man den Zugriff auf Rundfunksendungen kontrollieren? taschenbuch der telekom praxis 1996, Hrsg. Bernd Seiler, Schiele & Schön, Berlin 1996, oder J. Schwenk, Sicherheit bei Pay-TV. Proc. 2. ITG-Fachtagung Codierung für Quelle, Kanal und Übertragung.) Die Verschlüsselung der Inhalte stellt dabei eine sogenannte Leitungsverschlüsselung (Link Encryption) dar, bei der lediglich der Transportweg über Satellit verschlüsselt wird. Innerhalb des Transportweges, wie beispielsweise eines Übertragungskanals, ist dabei jedoch kein Schutz zwischen den auf den Übertragungskanal zugriffsberechtigten -Kunden selber gewährleistet, d.h. berechtigte Kunden können auf die Inhalte anderer Kunden (private E-Mails, HTML-Seiten) zugreifen.

Die neuen Medien Satellit und BK-Netz (und auch andere Medien wie z.B. terrestrischer Rundfunk, Passive optische Netze, PONs, ...) arbeiten im Gegensatz zum Telefonnetz nach dem Rundfunk-Prinzip, wobei Daten, die an einen Teilnehmer über diese Medien gesendet werden, auch andere Teilnehmer, die über dieses Medium angeschlossen sind, in gleicher Qualität erreichen. Im Folgenden soll der Übertragungsweg via Satellit stellvertretend für alle anderen Übertragungswege stehen. CA-Verfahren sind heute die einzigen praktisch eingesetzten Schlüsselmanagement-Verfahren, die in diesem Rundfunk-Szenario funktionieren.

Bei Internet-Diensten wie WWW, E-mail und FTP ist bekannt, dass die übertragenen Daten ungeschützt über das Internet übertragen werden. Bei sicherheitskritischen Anwendungen setzt man daher verschiedene Sicherheitstechniken ein, z.B. das von der Firma Netscape entwickelte „Secure Sockets Layer"-Protokoll für Homebanking, SSL. Angriffe auf die ungeschützten Daten im Internet erfordern aber zumindest ein geringes Expertenwissen und vor allem einen Zugang zu den Leitungen oder Vermittlungknoten

(Routern) im Internet. Diese Anforderungen werden nur von einem kleinen Personenkreis erfüllt. Dadurch ist es möglich, Angriffe auf ungeschützte Daten unter Strafe zu stellen.

Bei der Übertragung von Internet-Daten über ein Rundfunkmedium, beispielsweise mittels Satellit, können die übertragenen Daten von nicht berechtigten Personen mitgelesen werden. Geringe Kenntnisse über die Protokollschichten des Internet-Protocolls, IP, genügen, um den gesamten IP-Verkehr mitzuschneiden. (Als Analogon aus der bisherigen IP-Welt können die Sniffing-Angriffe auf den IP-Verkehr innerhalb eines Ethernt-LAN's angesehen werden. Hier braucht man nur die Ethernet-Karte in den „promiscous mode" umzuschalten und kann so den gesamten IP-Verkehr mitlesen. Die dazu benötigten Sniffer-Programme sind frei erhältlich und äußerst leicht zu bedienen.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren der eingangs genannten Art anzugeben, bei welchem der IP-Verkehr so über ein Rundfunkmedium übertragen wird, dass unbefugte Personen, die ebenfalls Zugriff auf das betreffende Rundfunkmedium bzw. den betreffenden Rundfunkkanal haben, den Dateninhalt nicht entschlüsseln können.

Die technische Aufgabe wird durch die im Kennzeichen des Patentanspruches 1 angegebenen Verfahrensmerkmale gelöst.

Das erfindungsgemäße Verfahren basiert auf der gesicherten Übertragung des IP-Verkehrs über Rundfunkmedien, wobei die ankommenden IP-Daten in DVB-Transportpakete, wie MPEG-2 Transport-Pakete aufgeteilt werden. MPEG-2 ist ein Internationaler Standard zur Kompression und Übertragung von digitalen Bewegtbildern nach der Norm ISO/IEC 13818. Diese Pakete werden dann auf Sendeseite von einem dedizierten Gerät, wie beispielsweise einem Multiplexer, MUX 4 oder einem separaten Scrambler, verschlüsselt, über die Rundfunkstrecke übertragen und auf der Empfangsseite von einem DVB-Empfangsgerät 6, wie beispielsweise einer Set-Top-Box STB, einer PC-Steckkarte oder einem DVB-Server in einem LAN, entschlüsselt. Die so erhaltenenen IP-Daten werden dann an die entsprechenden Geräte/Applikationen wie einen PC, einen Router oder einen TCP/IP-Stack) weitergegeben.

Das erfindungsgemäße Verfahren setzt das Vorhandensein eines Schlüsselmanagement-Systems wie beispielsweise ein Conditional-Access-System, CA-System und ein DVB-Empfangsgerät, wie beispielsweise eine Set-Top-Box oder entsprechenden PC-Steckkarten beim Kunden voraus. Der Kunde empfängt den IP-Verkehr über die Set-Top-Box oder die PC-Steckkarte beispielsweise von einem Satelliten 9. Der Rückkanal kann über Satellit 9 (BK-Netz), über Modem oder über ISDN realisiert sein.

Erfindungsgemäß wird vor der Übertragung der IP-Daten zum Kunden die Zieladresse (IP-Adresse bzw. TCP-Portnummer) des Anschlusses des Kunden

- erstens mit einem DVB-Service, der in der Service Information (SI) von DVB signalisiert wird und
- zweitens mit der eindeutigen Identifikationsnummer N der dem Kunden zugeordneten Empfangs-Komponente des CA-Systems 6a verknüpft.

Die Sende-Komponente des CA-Systems 3 sendet eine spezielle mit EMM (Entitle Management Message) bezeichnete Nachricht zur Freischaltung des DVB-Empfangsgerätes 6 des Kunden für den betreffenden DVB Service.

Der für die IP-Adresse ankommende IP-Verkehr wird vor der Übertragung über das Rundfunkmedium von einem IP-Encapsulator 2 in DVB-Empfangspakete, vorzugsweise MPEG-2-Transportpakete, aufgeteilt und mit den zugehörigen Kontrollnachrichten ECM´s verschlüsselt. Eine ECM (Entitlement Control Message) ist eine Nachricht, mit der neue Kontrollwörter übertragen und so Empfangsberechtigungen überprüft werden.

Liegt eine Freischaltung für das DVB-Empfangsgerät 6 vor, so gibt das Sicherheitsmodul das Kontrollwort zurück. Das Das DVB-Empfangsgerät 6 entschlüsselt die übertragenen DVB-Transportpakete, entpackt sie und leitet sie zum bestimmungsgemäßen Empfänger, wie beispielsweise einen PC 9, weiter.

Nachfolgend wird der konkrete Ablauf des Verfahrens näher erläutert:

1. Der PC 8 meldet sich über den Rückkanal bei einem IP-DVB-POP 5 an. Dabei muss er die eindeutige Identifikationsnummer N des CA-Sicherheitsmoduls 3 (d.h. der Chipkarte) mit angeben.
2. Vom IP-DVB-POP 5 erhält der PC sowohl eine temporäre IP-Adresse IP_X als auch eine temporäre DVB Service Nummer ID_Y zugewiesen.
3. Der IP-DVB-POP 5 teilt dem IP-Encapsulator 2 das aus der temporären IP-Adresse IP_X und der temporären DVB Service Nummer ID_Y bestehende Paar (IP_X, ID_Y) mit.
4. Der IP-Encapsulator 2 aktualisiert die von ihm generierten SI-Tabellen und weist der DVB Service Nummer ID_Y eine Paket Identifikations Nummer PID_Z zu. Der IP-Encapsulator 2 verpackt von nun an alle IP-Pakete mit Zieladresse IP_X in DVB-Pakete mit der Paket Identifikations Nummer PID_Z.
5. Der IP-DVB-POP 2 teilt der Sende-Komponente des CA-Systems 3 das aus der DVB Service Nummer ID_Y und der Identifikationsnummer N des CA-Sicherheitsmoduls 2 (d. h. der Chipkarte) bestehende Paar (ID_Y,N) mit.
6. Die Sende-Komponente des CA-Systems 3 generiert eine Freischalt-EMM für die Identifikationsnummer des Sicherheitsmoduls N und den Service mit der DVB Service Nr. ID_Y. Die Freischalt-EMM (Entitle Management Message) ist eine spezielle Nachricht zur Freischaltung des DVB-Empfangsgerätes 6, beispielsweise einer internen DVB PC-Karte oder einer externen Set Top Box STB. Auf Anforderung des Multiplexers MUX 4 generiert die Sende-Komponente des CA-Systems 3 Kontrollnachrichten, ECM's für den Service mit der DVB Service Nr. Y. Eine ECM, Entitlement Control Message, ist eine Nachricht mit der neue Kontrollwörter übertragen und Empfangsbestätigungen überprüft werden.

7. Der PC 8 veranlasst das DVB-Empfangsgerät 6, auf die DVB Service Nummer ID_Y umzuschalten. Das DVB-Empfangsgerät 6 empfängt die Freischalte-Nachricht EMM. Von nun an kann das DVB-Empfangsgerät 6 alle Kontrollnachrichten ECM's für den Service mit der DVB Service Nr. Y und somit auch den Service Y entschlüsseln.
8. Beim Abmelden des PC 8 oder nach einer bestimmten Ruhezeit wird die Assoziation (X,Y) durch den IP-DVB-POP 5 aufgehoben. Dies wird der Sende-Komponente des CA-Systems 3 und dem IP-Encapsulator 2 mitgeteilt.

Die Erfindung wird anhand eines Ausführungsbeispiels näher erläutert.

Fig. 1 zeigt ein Blockschaltbild zur Erläuterung des Verfahrens.

Dem Ausführungsbeispiel liegt die Annahme zugrunde, dass ein Kunde beispielsweise über das Internet ein sehr großes Software Paket mit einem Datenfile von ca.100 MByte erworben hat und es per Filetransfer FTP auf die Festplatte seines PC 8 laden möchte. Mit einer ISDN-Verbindung (64 kbit/s) würde der Filetransfer von ca. 100MByte etwa 3,472 Stunden dauern.

Wenn der Kunde den Filetransfer jedoch per Satellit 9 vornehmen würde, so könnte der Download von ca. 100 Mbyte in ca. 3,4 Minuten abgeschlossen sein. Das liegt darin begründet, dass dem Kunden zum Filetransfer per Satellit 9 kurzfristig eine Übertragungsrate von 4 Mbit/s zur Verfügung steht.

Der Kunde besitzt einen PC mit Satellitentuner und MPEG-2-Demultiplexer auf einer Einschubkarte. Der MPEG-2-Demultiplexer ist mit einer Satellitenantenne verbunden.

Bevor der Download startet, erscheint ein Dialog, bei dem der Kunde aufgefordert wird, einen Übertragungsweg zu wählen. Wählt er den Übertragungsweg Satellit 9, wird er in einem weiteren Fenster dazu aufgefordert, die Nummer seiner CA-Chipkarte einzugeben. Die Nummer der CA-Chipkarte ist nicht geheim.

Auf der Sendeseite wird dem FTP-Download ein DVB-Service und diesem Service ein Paket Identifikations Nummer PID_Z (Packet-Identifier) zugeordnet. Für diesen Service wird eine Freischaltungs-EMM generiert und an die angegebene Chipkartennummer (per Satellit 9 oder per Rückkanal) versandt. Optional kann hier Online noch einmal die Ankunft der Freischaltungs-EMM überprüft werden.

Der IP-Encapsulator 2 verpackt die IP-Pakete des FTP-Downloads in MPEG-2-Pakete mit der entsprechenden Paket Identifikations Nummer PID_Z. Die Sende-Komponente des CA-Systems 3 verschlüsselt die Pakete mit der Paket Identifikations Nummer PID_Z und generiert die zugehörigen Konrtrollnachrichten ECMs.

Die verschlüsselten Pakete werden per Satellit 9 übertragen. Durch die Verschlüsselung ist sichergestellt, dass der kostenpflichtige Inhalt nicht von Dritten empfangen werden kann.

Das setzt jedoch auch voraus, dass die Verschlüsselung für jeden Kunden individuell erfolgen muss. Das heißt, es genügt nicht für alle Kunden die gleiche Verschlüsselung einzusetzen, da alle anderen Kunden die Übertragung sonst einfach mitschneiden könnten.

Auf der Einsteckkarte im PC 8 des Kunden wurde bereits ein Filter gesetzt, der die zu dem DVB-Service gehörenden Kontrollnachrichten, ECM´s filtert und an die Chipkarte weiterleitet.

Die Chipkarte prüft, ob ein Recht zum Empfang dieses DVB-Service vorhanden ist und gibt ggf. den Sitzungsschlüssel an den Entschlüsselungsalgorithmus der PC-Steckkarte aus. Diese entschlüsselt die MPEG-2-Pakete, entpackt die darin enthaltenen IP-Pakete und leitet diese an den TCP/IP-Stack des PC 8 weiter.

Ab diesem Zeitpunkt kann der PC 8 nicht mehr unterscheiden, ob die IP-Pakete per Satellit 9 geliefert wurden oder per ISDN-Leitung.

Eine zweckmäßige Ausgestaltung des Verfahrens besteht darin, dass die Freischaltung per Freischaltungs EMM nicht länger als einen Tag gültig ist und dass eine DVB-Service-Nummer ID nur einmal pro Tag benutzt werden kann. Diese Maßnahmen tragen zur Erhöhung der Sicherheit des Verfahrens bei.

Bezugszeichenaufstellung:

1	Internet
2	IP-Encapsulator
3	Sende-Komponente des CA-Systems (Schlüsselmanagement-System)
4	Multiplexer / MUX
5	IP-DVB-POP
6	DVB-Empfangsgerät
6a	Empfangs-Komponente des CA-Systems
7	Rückkanal
8	PC
9	Satellit
N	Identifikationsnummer des Sicherheitsmoduls
IP_X	temporäre IP-Adresse
ID_Y	temporäre DVB Service Nummer
PID_Z	Paket Identifikations Nummer (Nummer zur Identifikation der Transportpakete)
ECM	Kontrollnachricht (Nachricht mit der neue Kontrollwörter übertragen und Empfangsberechtigungen überprüft werden)
EMM	Freischalte-Nachricht) (Nachricht mit der individuell neue Empfangsberechtigungen erteilt werden)
SI	Service-Information des DVB

Patentansprüche:

1. Verfahren zur abhörsicheren Bereitstellung vom IP-Diensten über ein Rundfunkmedium, bei dem der Kunde über ein DVB-Empfangsgerät (6) mit der Empfangs-Komponente eines CA Systems (6a) verfügt,
   dadurch gekennzeichnet, dass vor der Übertragung der IP-Daten zum Kunden die aus einer IP-Adresse bzw. einer TCP- Portnummer bestehenden Zieladresse des Anschlusses des Kunden
   a) mit einem DVB-Service, der in der Service Information (SI) vom DVB signalisiert wird und
   b) mit der eindeutigen Identifikationsnummer (N) der dem Kunden zugeordneten Empfangs-Komponente des CA-Systems (6a) verbunden wird,
   - dass die Sende-Komponente des CA-Systems (3) mittels einer Freischalte-Nachricht (EMM) eine Freischaltung für diesen DVB Service an die eindeutige Nummer der Empfangs–Komponente des CA-Systems (6a) sendet,
   - dass der für die IP-Adresse des Kunden ankommende IP-Verkehr von einem IP-Encapsulator (2) in DVB-Transportpakete des DVB-Services verpackt und mit den zugehörigen Kontrollnachrichten (ECM`s) versehen zum Kunden übertragen wird,
   - dass nach Verarbeitung der Kontrollnachrichten (ECM´s) und der Freischalte-Nachrichten (EMM`s) das DVB-Empfangsgerät (6) die DVB-Transportpakete entschlüsselt, die IP-Pakete entpackt und die entpackten IP-Pakete an das bestimmungsgemäße Endgerät, PC (8) des betreffenden Kunden weiterleitet.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet,
   - dass der Kunde sich mittels seines PC (8) über den Rückkanal (7) beim IP-DVB-POP (5) unter Angabe der eindeutige Identifikationsnummer des Sicherheits-moduls (N) der Empfangskomponente des CA-Systems (6a) anmeldet,
   - dass dem Kunden vom IP-DVB-POP (5) eine temporäre IP-Adresse (IP_X) und eine temporäre DVB Service Nummer (ID_Y) zugewiesen werden,

- dass der IP-DVB-POP (5) dem IP-Encapsulator (2) das aus der temporären IP-Adresse (IP_X) und der temporären DVB Service Nummer (ID_Y) bestehende Wertepaar (IP_X,ID_Y) mitteilt,
- dass der IP-Encapsulator (2) die von ihm generierten SI-Tabellen aktualisiert, der DVB Service Nummer (ID_Y) eine Paket Identifikations Nummer (PID_Z) zuweist und ab diesem Zeitpunkt alle IP-Pakete mit der Zieladresse (IP_X) in DVB-Transportpakete mit der Paket Identifikations Nummer (PID_Z) verpackt.
- dass der IP-DVB-POP (2) der Sende-Komponente des CA-Systems (3) das aus der temporären DVB Service Nummer (ID_Y) und der Identifikationsnummer des Sicherheitsmoduls N bestehende Wertepaar Paar (ID_Y,N) mitteilt,
- dass die Sende-Komponente des CA-Systems (3) eine Freischalte-Nachricht EMM

für die Identifikationsnummer des Sicherheitsmoduls (N) und die temporäre DVB

Service Nummer (ID_Y) generiert und dass auf Anforderung des Multiplexers (4) die Sende-Komponente des CA-Systems (3) Kontrollnachrichten (ECMs) für den Service mit der temporären DVB Service Nummer (ID_Y) generiert,

- dass der PC (8) das als interne DVB PC-Karte bzw. als externe Set Top Box STB ausgebildete DVB-Empfangsgerät (6) veranlasst, auf die temporäre DVB Service Nummer (ID_y) umzuschalten, und dass die interne DVB PC-Karte oder die externe Set Top Box die Freischalte-Nachricht (EMM) empfängt und damit in der

Lage ist, alle Kontrollnachrichten (ECM's) zur DVB Service Nummer (ID_Y) und somit auch den Service mit der temporären DVB Service Nummer ID_Y zu entschlüsseln, und

- dass beim Abmelden des PC (8) bzw. nach einer frei definierbaren Ruhezeit die Assoziation (IP_X,ID_Y) durch den IP-DVB-POP (5) wieder aufgehoben wird, und
- dass dieser Sachverhalt der Sende-Komponente des CA-Systems (3) und dem IP-Encapsulator (2) mitgeteilt wird.

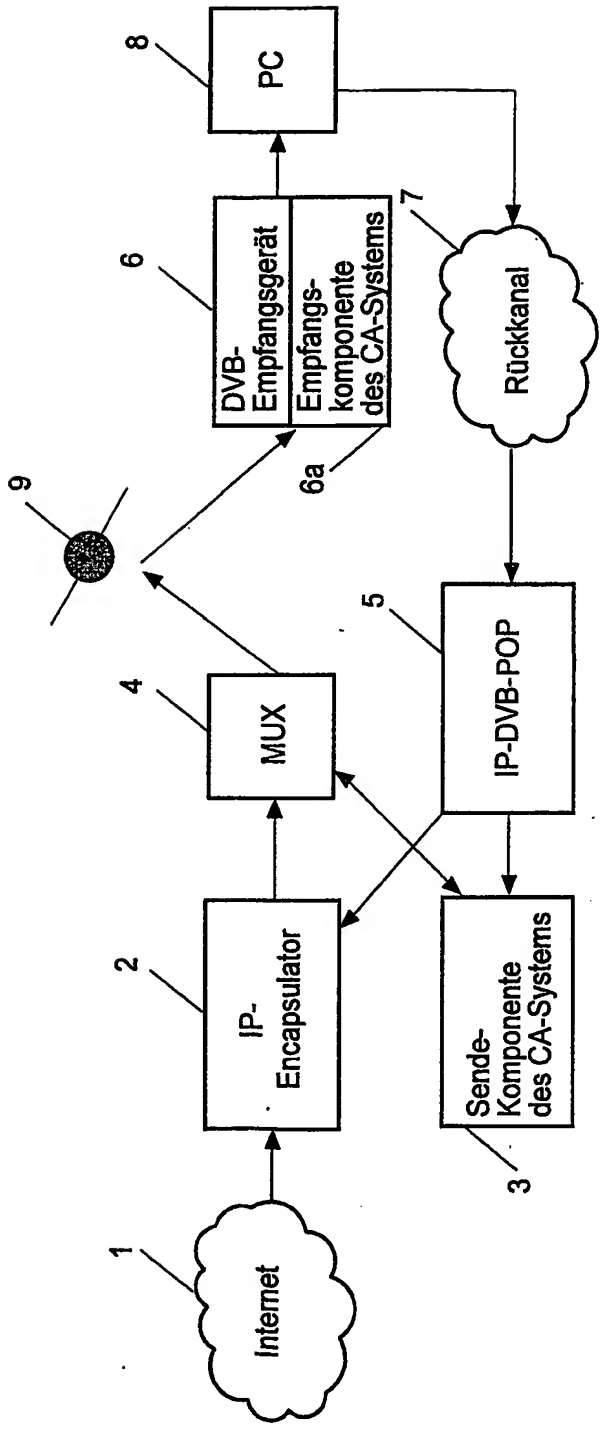

Internet
1
IP-
Encapsulator
2
Sende-
Komponente
des CA-Systems
3
MUX
4
IP-DVB-POP
5
DVB-
Empfangsgerät
Empfangs-
komponente
des CA-Systems
6
6a
Rückkanal
7
PC
8
9

Fig. 1

INTERNATIONAL SEARCH REPORT

Int nal Application No
PCT/EP 01/05343

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/24 H04N5/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	EP 1 022 884 A (CANAL PLUS SA) 26 July 2000 (2000-07-26) abstract paragraphs '0005!-'0008! paragraphs '0026!-'0028! paragraph '0041! paragraphs '0049!,'0050! paragraph '0057! paragraphs '0062!,'0063! paragraph '0068! paragraphs '0075!-'0078! paragraphs '0089!-'0091! --- -/--	1

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 October 2001	25/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Beaudet, J-P

INTERNATIONAL SEARCH REPORT

Int ial Application No
PCT/EP 01/05343

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" , EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE, NR. 266, PAGE(S) 64-77 XP000559450 ISSN: 0251-0936 paragraph '0003!	1
Y	WO 97 20413 A (NOKIA OY AB ;HAKULINEN HARRI (FI)) 5 June 1997 (1997-06-05) abstract page 3, line 20 -page 4, line 4 page 6, line 17 -page 7, line 28 page 11, line 29 -page 12, line 8	1
A	WO 99 37069 A (IRDETO BV ;WAJS ANDREW A (NL)) 22 July 1999 (1999-07-22) abstract page 1, line 17 - line 6 page 2, line 27 - line 32 page 3, line 16 - line 29	1,2
A	VAN SCHOONEVELD D: "Standardization of conditional access systems for digital pay television" , PHILIPS JOURNAL OF RESEARCH, ELSEVIER, AMSTERDAM, NL, VOL. 50, NR. 1, PAGE(S) 217-225 XP004008213 ISSN: 0165-5817 paragraphs '0002!,'0003!	1,2
A	STALLINGS W: "INTERNET ARMOR" , BYTE, MCGRAW-HILL INC. ST PETERBOROUGH, US, VOL. 21, NR. 12, PAGE(S) 127-128,130,132 XP000641459 ISSN: 0360-5280 the whole document	1,2

INTERNATIONAL SEARCH REPORT

ormation on patent family members

Inte onal Application No
PCT/EP 01/05343

Patent docum nt cited in search report		Publication date	Patent family member(s)		Publication date
EP 1022884	A	26-07-2000	EP	1022884 A1	26-07-2000
			AU	2124700 A	07-08-2000
			EP	1145524 A1	17-10-2001
			WO	0044145 A1	27-07-2000
WO 9720413	A	05-06-1997	FI	955773 A	31-05-1997
			AU	7698296 A	19-06-1997
			WO	9720413 A1	05-06-1997
WO 9937069	A	22-07-1999	AU	2618899 A	02-08-1999
			CN	1288629 T	21-03-2001
			WO	9937069 A1	22-07-1999
			EP	1048157 A1	02-11-2000

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 01/05343

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04N7/24 H04N5/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04N H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P,X	EP 1 022 884 A (CANAL PLUS SA) 26. Juli 2000 (2000-07-26) Zusammenfassung Absätze '0005!-'0008! Absätze '0026!-'0028! Absatz '0041! Absätze '0049!,'0050! Absatz '0057! Absätze '0062!,'0063! Absatz '0068! Absätze '0075!-'0078! Absätze '0089!-'0091! --- -/--	1

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
18. Oktober 2001	25/10/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax (+31–70) 340–3016	Beaudet, J-P

INTERNATIONALER RECHERCHENBERICHT

Internales Aktenzeichen
PCT/EP 01/05343

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" , EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE, NR. 266, PAGE(S) 64-77 XP000559450 ISSN: 0251-0936 Absatz '0003!	1
Y	WO 97 20413 A (NOKIA OY AB ;HAKULINEN HARRI (FI)) 5. Juni 1997 (1997-06-05) Zusammenfassung Seite 3, Zeile 20 -Seite 4, Zeile 4 Seite 6, Zeile 17 -Seite 7, Zeile 28 Seite 11, Zeile 29 -Seite 12, Zeile 8	1
A	WO 99 37069 A (IRDETO BV ;WAJS ANDREW A (NL)) 22. Juli 1999 (1999-07-22) Zusammenfassung Seite 1, Zeile 17 - Zeile 6 Seite 2, Zeile 27 - Zeile 32 Seite 3, Zeile 16 - Zeile 29	1,2
A	VAN SCHOONEVELD D: "Standardization of conditional access systems for digital pay television" , PHILIPS JOURNAL OF RESEARCH, ELSEVIER, AMSTERDAM, NL, VOL. 50, NR. 1, PAGE(S) 217-225 XP004008213 ISSN: 0165-5817 Absätze '0002!,'0003!	1,2
A	STALLINGS W: "INTERNET ARMOR" , BYTE, MCGRAW-HILL INC. ST PETERBOROUGH, US, VOL. 21, NR. 12, PAGE(S) 127-128,130,132 XP000641459 ISSN: 0360-5280 das ganze Dokument	1,2

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlich die zur selben Patentfamilie gehören

Inter ales Aktenzeichen
PCT/EP 01/05343

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 1022884	A	26-07-2000	EP	1022884 A1	26-07-2000
			AU	2124700 A	07-08-2000
			EP	1145524 A1	17-10-2001
			WO	0044145 A1	27-07-2000
WO 9720413	A	05-06-1997	FI	955773 A	31-05-1997
			AU	7698296 A	19-06-1997
			WO	9720413 A1	05-06-1997
WO 9937069	A	22-07-1999	AU	2618899 A	02-08-1999
			CN	1288629 T	21-03-2001
			WO	9937069 A1	22-07-1999
			EP	1048157 A1	02-11-2000